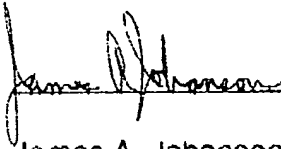## AFFIDAVIT UNDER 37 CFR 1.131

1.   I am an inventor for U.S. Patent Application 09/759,527.

2.   On March 31, 2000 I submitted an invention disclosure for company review. I hereby swear back under 37 CFR 1.131 to an invention date of no later than March 31, 2000 for the claimed invention.

3.   I declare under penalty of perjury that the foregoing is true and correct.

James A. Johanson   Date   Aug 3, 2004

MICROELECTRONICS PATENT COMMITTEE INVENTION SUBMISSION

Name(s) of Submitters	Telephone No:	Loc/Room	SBU/Org. Title:	HR ID:	E-Mail Address
Philip D. Mooney	610-709-1042	12B-239D	538870000	9116863	pdmooney@lucent.com
Joseph M. Cannon	610-709-1047	12B-239A	538870000	.4501920	cannon@lucent.com
James A. Johanson	610-709-1168	12B-129D	538870000	6899825	jjohanson@lucent.com
Date: 3/31/00					

TITLE: Enhanced Wireless Network Security Using GPS

Important Notes: (1) Keep in mind that your submission should be written so it can be understood in 5 to 10 minutes by a generalist. Avoid the use of undefined acronyms and jargon. Keep the language simple. (2) Have any of the above submitter(s) discussed this invention with, or provided an invention submission disclosing this invention to, an attorney other than the recipient of this invention submission?   ____YES   X NO

1. Describe the problem your invention solves:

Whereas a wired network connection affords a level of security in that the user must be *inside* a building in order to connect to the network, a wireless connection does not have the same restriction for access. A person just outside the building, but still in range of the wireless network (802.11, Bluetooth, etc) could gain access to an internal wireless server or device using stolen access codes. A stolen laptop could be used to steal data or files from the corporate network before the owner even could become aware of this transference.

2. Based on information of which you are already aware, describe:

(i) previous attempts to solve the problem your invention solves:

Dial up access uses multiple passwords or even constantly changing passwords to prevent unauthorized access.

(ii) the disadvantages of the previous attempts:

Does not address specific challenges of wireless access to secure servers. It would require all users inside the building to go through excessive, unnecessary security steps.

3. Summarize (30 words or less) the new feature(s) of your invention that solve the problem:

Access to a wireless network (e.g. for LAN access) is automatically restricted by requiring the mobile unit to provide GPS location when connected. A device whose GPS location is outside of the allowable area would be denied access or be required additional authorization steps.

4. Succinctly describe your invention, referring to drawings, sketches, photographs, etc., in sufficient detail to enable one knowledgeable in the invention's field of technology to understand construction and operation of the invention. Drawings, etc., should show only those features necessary for an understanding of the invention. Describe how/why your invention overcomes the disadvantages noted in 2. (ii) above.

While a computer, PDA or cell phone attempts to gain access to a service (such as a Bluetooth Printer or LAN access), the Bluetooth application passes its GPS location, accurate to a few meters (or even centimeters using Differential GPS), along with other profile required authentication information to the network. If the GPS location is within a preset area (or a

*** Provide the information requested in this box on each page of the submission, as well as drawings, sketches, photographs, etc. ***

Submitter(s) signature(s) and date: This invention submission has been read and
                                             understood by the following two witnesses:

_____ _____   _____ _____
                          date   date

_____ _____   _____ _____
                          date   date

_____ _____
                          date

relative distance), access is granted. If it is outside the preset area, access is denied or further authentication is required. See Figure 1.
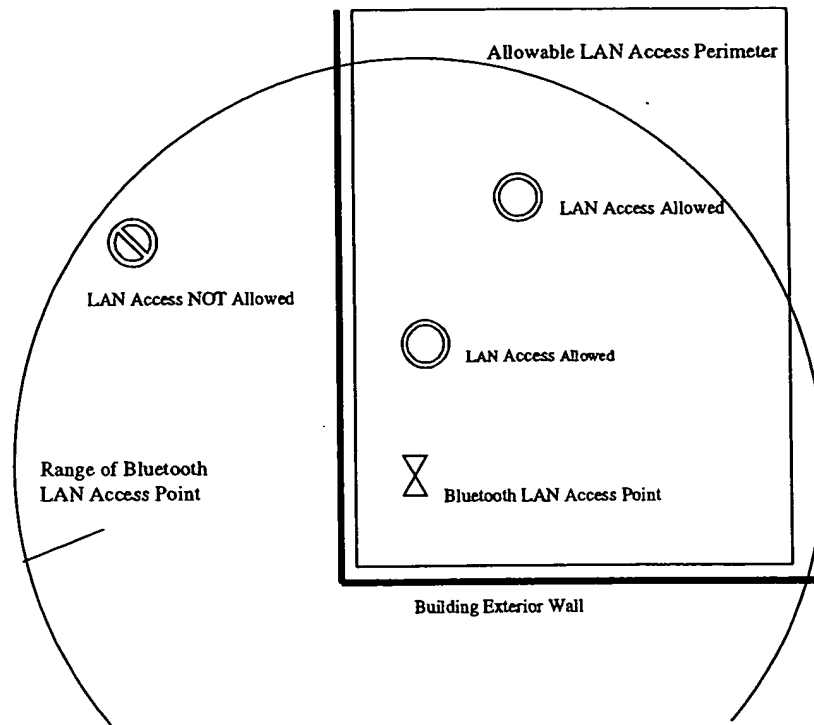

Figure 1 - Example using Wireless LAN Access

When a Bluetooth device discovers that there are multiple similar services within range, it could access the one that is physically closer to itself. Or using prior knowledge of walls or other obstacles, it could automatically access the service provider that is easier to get to.

Another use for GPS in a wireless piconet would be if you want your PDA to exchange business card information with others automatically, but only within the walls of a convention. This requirement could be an enhancement to the Generic Object Exchange Profile found in Bluetooth specifications. While you're down on the street getting a paper, you want your information to remain private. To setup the allowable area, you walk to each of the four corners of the allowable area and set the PDA. Or better yet, input the appropriate coordinates as published in the convention literature. Even better, your device receives the allowable coordinates for sharing business card information from a Bluetooth node at the entrance to the convention. Sharing of information could be based on your location or based on the GPS location of the one who is requesting your information. In addition, two devices could be programmed to automatically synchronize data or establish a connection only when within a predetermined range.

5. Advantages of your invention:
- Additional security for wireless network connections.

*** Provide the information requested in this box on each page of the submission, as well as drawings, sketches, photographs, etc. ***

Submitter(s) signature(s) and date: This invention submission has been read and
                                                       understood by the following two witnesses:

_____   _____   _____   _____
                             date   date

_____   _____   _____   _____
                             date   date

_____   _____
                             date

- Requires no additional user input or hassle.
- Greater control over privacy of information.
- Adds distinctiveness and value to Lucent ME's chips.
- Gives device manufacturer added capability beyond essential Bluetooth.
- Integrating the GPS into the wireless chips would reduce the chance of faking out the authentication process.
- Could use GPS or any other location finding technology (e.g. cell tower triangulation).
- Allows control of autonomous events like file synchronization.
- Either actual location or relative distance could be used for access.

6. Explain how use of your invention would be detected:
Would be advertised in packaging and marketing materials.

7. References

http://www.trimble.com/gps/howgps/gpsfram2.htm